**PRE-APPEAL BRIEF REQUEST
FOR REVIEW****MAIL STOP AF**

COMMISSIONER FOR PATENTS

P.O. Box 1450

ALEXANDRIA, VA 22313-1450

Application Number	10/679,371
Filing Date	October 7, 2003
First Named Inventor	Anthony C. FASCENDA
Art Unit	2131
Examiner Name	Shin Hon CHEN
Attorney Docket No.	72167.000176

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this appeal.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided

I am the:

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96).

☒ Attorney or Agent of Record 51,184
(Reg. No.)

☐ Attorney or Agent acting under 37 CFR 1.34.
Registration No. if acting under 37 CFR 1.34 _____


SignatureJeffrey Scott Leaning

Typed or printed name

(202) 419-2092

Requester's telephone number

March 14, 2006

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number : 10/679,371 Confirmation No.: 4292
Applicant : Anthony C. FASCENDA
Filed : October 7, 2003
Title : LOCALIZED NETWORK AUTHENTICATION AND SECURITY
USING TAMPER-RESISTANT KEYS
TC/Art Unit : 2131
Examiner: : Shin Hon Chen
Docket No. : 62922.000003
Customer No. : 21967

MAIL STOP AF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

The following is responsive to the Office Action mailed on November 14, 2005 ("Office Action"). Claims 1-11 and 13-28 are pending in the present application. Claims 1-11, 13 and 19-28 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over U.S. Patent No. 6,397,328 to Pitchenik *et al.* ("Pitchenik") in view of U.S. Patent No. 5,473,689 to Eberhard ("Eberhard"). Claims 13 and 14 stand rejected over Pitchenik in view of Eberhard and further in view of U.S. Published Application No. 2004/0203590 to Shteyn ("Shteyn"). Applicants respectfully requests that the members of the Pre-Appeal Brief Conference (the "Conference") allow all pending claims in view of the following remarks.

I. The Office Action Impermissibly Combines Multiple Embodiments Of The Cited Art

Different embodiments in the same reference may not be combined piecemeal to form a rejection under 35 U.S.C. § 102. However, the Office Action repeatedly cites portions of Pitchenik that disclose multiple embodiments. Regarding claim 1, for example, the Office Action cites Pitchenik, col. 2, l. 40 - col. 3, l. 28 and col. 4, ll. 32-67. These passages refer to no less than seven (7) different embodiments:

The present invention provides a method for verifying that a host system is the expected host system once the PSD has been verified as the expected PSD. ...

The present invention further provides alternate embodiments secure and reliable methods for verifying in the host system that the expected PSD is coupled to the host system. In one embodiment, a message, such as a random number, is generated in the Host system and sent to the PSD. In one embodiment, the PSD

encrypts the number and transmits it to the Host system. ... In an alternate embodiment, the random number is signed in the PSD. ...

In yet another embodiment, the PSD has a private key which is associated with a specific public key that is stored in the host PC. ...

In another embodiment, a random number is generated in the host system and encrypted with a PSD state identification number. ...

Pitchenik, col. 2, l. 40 - col. 3, l. 28 (emphasis added). The rejections of independent claims 13 and 19 contain similar citations. In order to support a rejection under 35 U.S.C. § 102, every element of the claimed invention must be literally present, arranged as in the claim. See *Perkin-Elmer Corp. v. Computervision Corp.*, 732 F.2d 888, 894, 221 USPQ at 673 (Fed. Cir. 1984); *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 771-72, 218 USPQ 781, 789 (Fed. Cir. 1983).

Applicants have now twice explicitly requested that the Examiner specify exactly which single embodiment is relied upon in forming the rejection under § 102. See Response to Office Action filed March 23, 2005, page 5, (III); Response to Office Action filed August 23, 2005, page 8 (“Applicant reiterates the request that the Examiner specify exactly which single embodiment of the cited reference is relied upon in forming any rejection under § 102.”). Applicants are now forced to turn to the Conference to withdraw this clearly improper rejection.

For completeness, Applicants note that no Pitchenik embodiment anticipates or renders obvious the present invention as claimed, whether alone or in combination with the other cited references. As such, the rejection is clearly improper, and Applicants respectfully request that the Conference withdraw the rejections and pass the claims to issue.

II. The Office Action Fails To Provide Proper Motivation To Combine

The Office Action offers nothing but conclusory, unsupported statements as its alleged motivation to combine references in its rejection of independent claims 1, 13 and 19.

Regarding claims 1, 13 and 19, the Examiner concedes that Pitchenik does not disclose “generating a second random number, wherein the second random number is different from the first random number.” Office Action, page 3. The Examiner turns to Eberhard as allegedly filling the gap. In particular, the Office Action presents the following alleged motivation to combine Eberhard with Pitchenik:

[1] It would have been obvious to one having ordinary skill in the art to generate different random numbers when two devices try to authenticate each other.

[2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant’s invention to combine the teachings of Eberhard within the system of Pitchenik because using two random numbers allows both devices to exclusively authenticate each other.

Office Action, pages 3, 4 and 8. Applicants assert that [1] is, at best, a conclusory statement that assumes what it purports to prove. Moreover, [1] is merely a paraphrased version of the claim limitation at issue together a word taken from the claim preamble. There is no indication in any art cited in the Office Action that Pitchenik should be combined with Eberhard. Further, [2], in a

conclusory manner, states that a combination of Pitchenik with Eberhard would have been obvious by relying on what is essentially a re-statement of [1]. That is, [2] is a conclusory statement that uses the conclusory statement [1] as its justification. This alleged motivation to combine cannot stand. The U.S. Patent Office cannot simply restate a claim limitation as grounds for combining references used to reject the claim at issue. The Office Action simply fails to provide proper motivation to combine Pitchenik with Eberhard in rejecting claims 1, 13 and 19. As such, Applicants respectfully request that the Conference withdraw the rejections of claims 1, 13, 19 and all claims dependent thereon.

Regarding claim 13, the Office Action concedes that Pitchenik fails to disclose that “each tamper-resistant physical token is removable.” Office Action, page 8. Turning to Shteyn as allegedly filing the gap, the Examiner writes:

[1] It would have been obvious to one having ordinary skill in the art to store identifications information and cryptographic key into the hardware key while authentication takes place between a mobile terminal and an access point.
[2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shteyn within the combination of Pitchenik-Eberhard because dongle is well known in the art for providing security parameters within network.

Office Action, page 9. Here again, [1] is no more than a conclusory statement that assumes what it purports to prove. There is no reasoning as to why “it would have been obvious,” only a bare statement that it would have been. Moreover, neither the present claims nor the disclosure of Pitchenik are directed to a “mobile terminal and an access point.” As such, it is improper to use the same as justification for any alleged obviousness. As to [2], this statement is at best a conclusory shotgun assertion that is unsupported by any art of record. As such, neither [1] nor [2] are proper motivation for combining Pitchenik with Shteyn. Accordingly, Applicants respectfully request that the Conference withdraw the rejections of claim 13 and all claims dependent thereon.

III. The Cited Reference Fail to Disclose A Physical Token As Claimed

Claim 13 as amended recites a “removable unique tamper-resistant physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number.” In order to assist the Conference's analysis, Applicants note that the Office Action rejects claim 13 over Pitchnick in view of Eberhard and further in view of Shteyn as follows: The Office Action relies on Pitchenik as disclosing each limitation of claim 13 except: (1) “generat[ing] at least one random number different from a received random number,” for which the Office Action relies on Eberhard; and (2) the physical token being “removable,” for which the Office Action relies on Shteyn. Other than these two enumerated instances, the Office Action relies on Pitchenik as allegedly disclosing every limitation of claim 13. In particular, it is the position of the Examiner that Pitchenik discloses a “physical token.” See Office Action mailed May 26, 2005, page 10.

A. Pitchenik Fails To Disclose A “Physical Token”

The Office Action relies on Pitchenik as disclosing a physical token. However, Pitchenik has absolutely no teaching, suggestion, consideration, discussion, or reference concerning a “physical

token.” The present specification discusses the qualities of a physical token: “[t]he present invention [uses] ... physical keys in the form of easy-to-use adapters that attach to existing computing devices and wireless access points... These physical keys are secure, tamper-resistant physical tokens.” Present application, paragraph 36. Pitchenik lacks any discussion of such physical tokens.

As best understood, the Examiner’s position appears to be that the “physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number” is included somewhere in Pitchnik’s Postage Security Device (“PSD”). The Examiner stakes out this position as follows:

[A]pplicant argues that Pitchenik reference does not disclose a tamper resistant physical token. However, Pitchenik discloses that the cryptographic key and unique ID are stored within the postage security device, which is a tamper resistant device. Therefore, the tamper-resistant physical token is included in the postage security device ready for authentication.

Office Action mailed May 26, 2005, page 10. This position is untenable. Surely the examiner does not argue that any key together with an ID constitute a “physical token,” no matter where or how these items are stored. The mere fact that Pitchenik stores a key and an ID somewhere in a PSD does not mean that that the storage location is a “physical token.” Pitchenik could, for example, store a key and an ID on a permanent hard drive inside the PSD. Such a permanent hard drive is not a “removable physical token.”

In short, the mere fact that Pitchenick discloses that a key and ID are located somewhere inside a PSD box does not anticipate “at least one authentication device, wherein each authentication device includes a removable unique tamper-resistant physical token comprising a random number generator configured to generate at least one random number different from a received random number.”

B. Pitchenik Fails To Disclose A “Tamper-Resistant” Physical Token

Pitchenik has absolutely no teaching, suggestion, consideration, discussion, or reference concerning anything that is “tamper-resistant.” At most, Pitchenik discloses in a completely generic manner that the entire system is “secure.” See Pitchenik, column 1, lines 51-53. Applicants strongly dispute that a generic disclosure of an entire system being “secure” amounts to a disclosure of a “physical token” being “tamper-resistant.” “Secure” does not imply “tamper-resistant.” For example, encrypted data stored on magnetic media might be considered “secure,” but are certainly not “tamper-resistant” because such data could easily be altered. In short, “secure” does not mean or imply “tamper-resistant.”

Furthermore, Pitchenik does not disclose any physical token being tamper-resistant. Rather, the entire system of Pitchenik is referred to as being “secure,” although exactly how the system is “secure” is not specified. See Pitchenik, column 2, lines 34-39. The disclosure of Pitchenik cannot, therefore, be properly relied upon to reject claim 13, which specifies that the physical token is “tamper-resistant.” Because Pitchenik lacks any teaching regarding a “unique tamper-resistant physical token,” the rejection is improper and should be withdrawn.

C. Shteyn Fails To Disclose A Physical Token As Claimed

The Office Action relies on Shteyn as allegedly disclosing a “removable” physical token. The Examiner states that “Shteyn discloses using a dongle installed via a USB to secure communications in a wireless network.” Office Action, pages 8-9. However, Shteyn’s dongle is not “tamper-resistant.” Shteyn’s dongle does not contain a “random number generator.” Shteyn’s dongle does not contain “a unique secret cryptographic key.” And Shteyn’s dongle does not include “a unique serial number.” See Shteyn, paragraph 27. Thus, Shteyn cannot properly be relied upon to remedy that Pitchenik fails to disclose these limitations. A generic reference to “using a dongle for authentication purposes” does not amount to a teaching of a “removable unique tamper-resistant physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number.” In the complete absence of such disclosure, any reliance on Shteyn is misplaced. Applicant accordingly requests that the rejection be withdrawn.

Because neither Pitchenik nor Shteyn disclose a “removable unique tamper-resistant physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number,” the rejections of claim 13 and all claims dependent thereon are improper and must be withdrawn.

IV. Conclusion

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. Applicants respectfully request that the Conference hold that the claims are allowable.

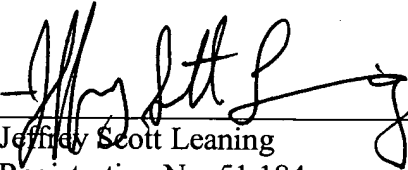
In the event that a variant exists between the amount tendered and that determined by the U.S. Patent and Trademark Office to enter the present Arguments, the associated Pre-Appeal Brief Request For Review, the Notice Of Appeal, or to maintain the present application pending, please charge or credit such variance to the undersigned’s Deposit Account No. 50-0206.

Respectfully submitted,

HUNTON & WILLIAMS LLP

Dated: March 14, 2006

By:


Jeffrey Scott Leaning
Registration No. 51,184

Hunton & Williams LLP
Intellectual Property Department
1900 K Street, N.W., Suite 1200
Washington, DC 20006-1109
(202) 419-2092 (telephone)
(202) 778-2201 (facsimile)

JSL:mia